CLAIMS

What is claimed is:

1. A method for authenticating a client within a distributed data processing system, the method comprising the steps of:

receiving a digital certificate from the client at a host within the distributed data processing system;

obtaining a host identity for the client from the digital certificate;

retrieving host-encrypted secret data associated with the host identity from the digital certificate;

decrypting the host-encrypted secret data with a host private key; and

authenticating the client using the host identity and the decrypted secret data.

2. The method of claim 1, wherein the host acts as a proxy for the client.

3. The method of claim 1 further comprising:

verifying the received digital certificate.

4. The method of claim 1 further comprising:

generating, at the client, a request for a digital certificate comprising host identity mapping data;

sending the request for the digital certificate to a certifying authority (CA); and

receiving a digital certificate comprising host identity mapping data from the certifying authority.

5. The method of claim 4 further comprising:

storing the host identity in the request for the digital certificate;

encrypting secret data associated with the host identity using a public key of the certifying authority to generate CA-encrypted secret data; and

storing the CA-encrypted secret data in the request for the digital certificate, wherein the host identity and the CA-encrypted secret data comprise the host identity mapping data in the request for the digital certificate.

6. The method of claim 4 further comprising:

receiving, at the certifying authority, the request for a digital certificate;

generating the digital certificate in response to the received request for the digital certificate; and

sending the generated digital certificate to the client.

7. The method of claim 4 further comprising:

retrieving CA-encrypted secret data from the host identity mapping data in the request for the digital certificate;

decrypting the CA-encrypted secret data associated with the host identity using a private key of the certifying authority to generate decrypted secret data;

encrypting the decrypted secret data associated with the host identity using a public key of the host to generate the host-encrypted secret data; and

storing the host-encrypted secret data in the digital certificate, wherein the host identity and the host-encrypted secret data comprise the host identity mapping data in the digital certificate.

8. The method of claim 1 wherein the digital certificate comprises multiple host identities for multiple hosts within the distributed data processing system.

9. The method of claim 1 wherein the digital certificate is formatted according to the X.509 standard.

10. The method of claim 9 wherein the host identity and the host-encrypted secret data associated with the host identity is stored within an X.509 extension within the digital certificate.

11. The method of claim 1 further comprising:

performing multiple authentication processes within the distributed data processing system for the client through the host using information within the digital certificate.

12. A method for generating a digital certificate, the method comprising the steps of:

receiving, at a certifying authority (CA), a request for a digital certificate from a client, wherein the request for a digital certificate comprises host identity mapping data;

generating the digital certificate in response to the received request for a digital certificate; and

sending the generated digital certificate to the client, wherein the digital certificate comprises host identity mapping data from the certifying authority.

13. The method of claim 12 further comprising:

retrieving CA-encrypted secret data from the host identity mapping data in the request for a digital certificate;

decrypting the CA-encrypted secret data associated with a host identity using a private key of the certifying authority to generate decrypted secret data;

encrypting the decrypted secret data associated with the host identity using a public key of a host to generate a host-encrypted secret data; and

storing the host-encrypted secret data in the digital certificate, wherein the host identity and the host-encrypted secret data comprise the host identity mapping data in the digital certificate.

14. An apparatus for authenticating a client within a distributed data processing system, the apparatus comprising:

first receiving means for receiving a digital certificate from the client at a host within the distributed data processing system;

obtaining means for obtaining a host identity for the client from the digital certificate;

first retrieving means for retrieving host-encrypted secret data associated with the host identity from the digital certificate;

first decrypting means for decrypting the host-encrypted secret data with a host private key; and

authenticating means for authenticating the client using the host identity and the decrypted secret data.

15. The apparatus of claim 14, wherein the host acts as a proxy for the client.

16. The apparatus of claim 14 further comprising:

verifying means for verifying the received digital certificate.

17. The apparatus of claim 14 further comprising:

first generating means for generating, at the client, a request for a digital certificate comprising host identity mapping data;

first sending means for sending the request for the digital certificate to a certifying authority (CA); and

second receiving means for receiving a digital certificate comprising host identity mapping data from the certifying authority.

18. The apparatus of claim 17 further comprising:

first storing means for storing the host identity in the request for the digital certificate;

first encrypting means for encrypting secret data associated with the host identity using a public key of the certifying authority to generate CA-encrypted secret data; and

second storing means for storing the CA-encrypted secret data in the request for the digital certificate, wherein the host identity and the CA-encrypted secret data comprise the host identity mapping data in the request for the digital certificate.

19. The apparatus of claim 17 further comprising:

third receiving means for receiving, at the certifying authority, the request for a digital certificate;

second generating means for generating the digital certificate in response to the received request for the digital certificate; and

second sending means for sending the generated digital certificate to the client.

20. The apparatus of claim 17 further comprising:

second retrieving means for retrieving CA-encrypted secret data from the host identity mapping data in the request for the digital certificate;

second decrypting means for decrypting the CA-encrypted secret data associated with the host identity using a private key of the certifying authority to generate decrypted secret data;

second encrypting means for encrypting the decrypted secret data associated with the host identity using a public key of the host to generate the host-encrypted secret data; and

third storing means for storing the host-encrypted secret data in the digital certificate, wherein the host identity and the host-encrypted secret data comprise the host identity mapping data in the digital certificate.

21. The apparatus of claim 14 wherein the digital certificate comprises multiple host identities for multiple hosts within the distributed data processing system.

22. The apparatus of claim 14 wherein the digital certificate is formatted according to the X.509 standard.

23. The apparatus of claim 22 wherein the host identity and the host-encrypted secret data associated with the host identity is stored within an X.509 extension within the digital certificate.

24. The apparatus of claim 14 further comprising:

performing means for performing multiple authentication processes within the distributed data processing system for the client through the host using information within the digital certificate.

25. An apparatus for generating a digital certificate, the apparatus comprising:

receiving means for receiving, at a certifying authority (CA), a request for a digital certificate from a client, wherein the request for a digital certificate comprises host identity mapping data;

generating means for generating the digital certificate in response to the received request for a digital certificate; and

sending means for sending the generated digital certificate to the client, wherein the digital certificate comprises host identity mapping data from the certifying authority.

26. The apparatus of claim 25 further comprising:

retrieving means for retrieving CA-encrypted secret data from the host identity mapping data in the request for a digital certificate;

decrypting means for decrypting the CA-encrypted secret data associated with a host identity using a private key of the certifying authority to generate decrypted secret data;

encrypting means for encrypting the decrypted secret data associated with the host identity using a public key of a host to generate a host-encrypted secret data; and

storing means for storing the host-encrypted secret data in the digital certificate, wherein the host identity and the host-encrypted secret data comprise the host identity mapping data in the digital certificate.

27. A computer program product on a computer readable medium for use in a distributed data processing system for authenticating a client, the computer program product comprising:

instructions for receiving a digital certificate from the client at a host within the distributed data processing system;

instructions for obtaining a host identity for the client from the digital certificate;

instructions for retrieving host-encrypted secret data associated with the host identity from the digital certificate;

instructions for decrypting the host-encrypted secret data with a host private key; and

instructions for authenticating the client using the host identity and the decrypted secret data.

28. The computer program product of claim 27, wherein the host acts as a proxy for the client.

29. The computer program product of claim 27 further comprising:

instructions for verifying the received digital certificate.

30. The computer program product of claim 27 further comprising:

instructions for generating, at the client, a request for a digital certificate comprising host identity mapping data;

instructions for sending the request for the digital certificate to a certifying authority (CA); and instructions for receiving a digital certificate comprising host identity mapping data from the certifying authority.

31. The computer program product of claim 30 further comprising:

instructions for storing the host identity in the request for the digital certificate;

instructions for encrypting secret data associated with the host identity using a public key of the certifying authority to generate CA-encrypted secret data; and

instructions for storing the CA-encrypted secret data in the request for the digital certificate, wherein the host identity and the CA-encrypted secret data comprise the host identity mapping data in the request for the digital certificate.

32. The computer program product of claim 30 further comprising:

instructions for receiving, at the certifying authority, the request for a digital certificate;

instructions for generating the digital certificate in response to the received request for the digital certificate; and

instructions for sending the generated digital certificate to the client.

33. The computer program product of claim 30 further comprising:

instructions for retrieving CA-encrypted secret data from the host identity mapping data in the request for the digital certificate;

instructions for decrypting the CA-encrypted secret data associated with the host identity using a private key of the certifying authority to generate decrypted secret data;

instructions for encrypting the decrypted secret data associated with the host identity using a public key of the host to generate the host-encrypted secret data; and

instructions for storing the host-encrypted secret data in the digital certificate, wherein the host identity and the host-encrypted secret data comprise the host identity mapping data in the digital certificate.

34. The computer program product of claim 27 wherein the digital certificate comprises multiple host identities for multiple hosts within the distributed data processing system.

35. The computer program product of claim 27 wherein the digital certificate is formatted according to the X.509 standard.

36. The computer program product of claim 35 wherein the host identity and the host-encrypted secret data associated with the host identity is stored within an X.509 extension within the digital certificate.

37. The computer program product of claim 27 further comprising:

instructions for performing multiple authentication processes within the distributed data processing system for the client through the host using information within the digital certificate.

38. A computer program product on a computer readable medium for use in a distributed data processing system for generating a digital certificate, the computer program product comprising:

instructions for receiving, at a certifying authority (CA), a request for a digital certificate from a client, wherein the request for a digital certificate comprises host identity mapping data;

instructions for generating the digital certificate in response to the received request for a digital certificate; and

instructions for sending the generated digital certificate to the client, wherein the digital certificate comprises host identity mapping data from the certifying authority.

39. The computer program product of claim 38 further comprising:

instructions for retrieving CA-encrypted secret data from the host identity mapping data in the request for a digital certificate;

instructions for decrypting the CA-encrypted secret data associated with a host identity using a private key of the certifying authority to generate decrypted secret data;

instructions for encrypting the decrypted secret data associated with the host identity using a public key of a host to generate a host-encrypted secret data; and

instructions for storing the host-encrypted secret data in the digital certificate, wherein the host identity and the host-encrypted secret data comprise the host identity mapping data in the digital certificate.

40. A data structure representing a digital certificate for use in a data processing system, the data structure comprising:

an issuer name;

a signature;

a subject name; and

an extension, wherein the extension comprises a host identity and host-encrypted secret data associated with the host identity.